Theorems on the Groups of Isomorphisms of Certain Groups.

By Louis Clark Mathewson.

Introduction.

The properties of the group of isomorphisms of a group are such that the importance of these groups is being widely recognized. The theory of the group of isomorphisms includes the theory of primitive roots,* Fermat's and Wilson's theorem,† the determination of the various groups of which a given group is an invariant subgroup,‡ and the solvability of equations by means of radicals. Because of the numerous uses, and since only a limited amount of theory has been developed, this paper has for its object the presentation of several theorems bearing on the groups of isomorphisms of certain familiar groups.

The theory of an isomorphism between two different groups, which is indispensably connected with the complete determination of the intransitive groups of a given degree,§ seems to have been studied first. In general, two groups are said to be isomorphic, if to each operator of the first there corresponds one or more operators of the second, and *vice versa*, in such a way that to the product of any two operators of the first corresponds the product of the corresponding operators of the second. If the correspondence is $1:1$, the isomorphism is termed *simple*; if $a:1$, it is called *multiple*. The importance of the idea of simple isomorphism between two groups lies in the fact that abstractly two such groups have the same properties; that is, both are simple or both composite, abelian or non-abelian, etc. In 1868 Jordan introduced and defined an $a:1$-isomorphism,|| and ten years later Capelli gave the generalized idea of an $a:b$-isomorphism.¶ Others who have studied these isomorphisms are Netto, Maillet, Dyck, Weber, Miller, Burnside, Dickson, etc.

---

* Miller, *Bulletin of American Mathematical Society* (2), Vol. VII (1900–01), p. 350.

† Miller, *Philosophical Magazine*, Vol. CCXXXI (1908), p. 224; *Transactions of American Mathematical Society*, Vol. IV (1903), p. 158; *Annals of Mathematics*, Vol. IV (1903), p. 188.

‡ Burnside, "Theory of Groups," 1897, § 165.

§ For a detailed discussion see Bolza, American Journal of Mathematics, Vol. XI (1889), pp. 195–214.

|| *Comptes Rendus Acad. Sc. Paris*, Vol. LXVI (1868), p. 836.

¶ *Giornali di Matematiche*, Vol. XVI (1878), p. 33.

The theory of the group of isomorphisms of a group with itself had its genesis, like most other extensive theories of science, in the discovery and study of isolated cases, and some of these cases seem to have been worked out before it was realized that every finite group has a single group of isomorphisms which also is of finite order. Betti credits Galois with having given without proof an expression for the group of isomorphisms of a group of order p^m,* and Dickson makes a comment upon Betti's remark† and refers to a fragment of a posthumous paper, "Des équations primitives qui sont soluble par radicaux."‡ In his own paper Betti obtains his "massimo moltiplicatore" of the cyclic group of order p^m. Jordan took the next step by starting with the abelian transitive linear group defined by $x_i' \equiv x_i + a_i$ $(i=1, \ldots, n)$, and found the non-homogeneous linear group as the largest group of linear substitutions under which the given group is invariant.§ Other special cases were observed by Gierster|| and Klein.¶ As applied to finite abstract groups, the conception of the group of isomorphisms was developed by Hölder** and by Moore†† independently of each other.‡‡

If a group G be written twice with 1:1-correspondence between its operators such that to the product of two operators of the first arrangement corresponds the product of the two corresponding operators in the second arrangement, the group is said to be *simply isomorphic with itself.*§§ Frobenius has called this an *automorphism,*|||| while Miller has employed the term *holomorphism.*¶¶ If G be written as a regular substitution group, then operators on the same letters exist which transform it according to any of these simple isomorphisms.*** If any isomorphism is effected by an operator of G itself, the isomorphism is called *cogredient* or *inner*; all others are called *contragredient* or *outer.* In his article of 1893 Hölder first proved that "the totality of the different isomorphisms of a group with itself form a group I,"††† and later states that the cogredient isomorphisms always form an invariant sub-

* *Annali di Scienze Matematiche e Fisiche,* Vol. VI (1855), p. 34.

† *Transactions of American Mathematical Society,* Vol. I (1900), p. 30, foot-note.

‡ "Oeuvres Mathématiques D'Evariste Galois," 1897, p. 58.

§ Traité des Substitutions, 1870, §§ 118, 119.

|| *Mathematische Annalen,* Vol. XVIII (1881), p. 354.

¶ "Vorlesungen über das Ikosaeder," 1884, p. 232.

** *Mathematische Annalen,* Vol. XLIII (1893), pp. 313 *et seq.*

†† *Bulletin of American Mathematical Society,* Vol. I (1894–95), p. 61.

‡‡ *Bulletin of American Mathematical Society,* Vol. II (1895–96), p. 33, foot-note.

§§ Cf. Burnside, "Theory of Groups," 1911, p. 81.

|||| *Sizungsberichte der Berliner Akademie,* 1901, p. 1324.

¶¶ *Bulletin of American Mathematical Society* (2), Vol. IX (1902), p. 112.

*** Frobenius, *Berliner Sizungsberichte,* 1895, pp. 184, 185.

††† *Mathematische Annalen,* Vol. XLIII (1893), p. 314.

group of this group of isomorphisms I.* It is readily seen that the group of cogredient isomorphisms is simply isomorphic with the quotient of the given group with respect to its central,† and if the given group G has no invariant operators besides the identity, the group of cogredient isomorphisms is simply isomorphic with G itself. If G has no invariant operator besides the identity and admits of no contragredient isomorphism, Hölder has called it a *complete* group, and has proved explicitly that the symmetrical group of degree n ($n > 2$, $n \neq 6$) is a complete group.* Frobenius defines as *characteristic* any operator or subgroup of a given group G which is transformed into itself by all the operators of the group of isomorphisms of G;‡ and Burnside has introduced the term *holomorph*, to mean the group composed of all the substitutions on the letters of a regular substitution group G which transform G into itself.§

Following the developments made by the two pioneers in the theory of the group of isomorphisms of a group, more general work began and applications of the theory were made. Burnside's "Theory of Groups" (1897) was the first text-book to elaborate the theory; Miller determined the groups of isomorphisms of all the substitution groups of degree less than 8, in connection with which he proved several far-reaching theorems.|| In all, upwards of forty articles have appeared in mathematical literature on isomorphisms of a group or on properties of the group of isomorphisms of a group. Many of these have been written by Miller, most of the others being by Burnside, Dickson and Moore, who have been mentioned previously, and by Young (J. W.) and Ranum.

I. *Theorems on Certain Groups Involving a Characteristic Set.*

DEFINITION. *A characteristic set in a group G consists of one or more complete sets of conjugates under the group of isomorphisms of G.*

This definition includes the notion of a characteristic set of operators of G as well as that of a characteristic set of subgroups of G. The distinguishing property in a characteristic set, either of operators or of subgroups, is thus seen to be that the set contains a definite number of operators which as an aggregate correspond among themselves in all the isomorphisms of G. If a characteristic set consists of but two conjugates, it may be called a character-

---

* *Mathematische Annalen*, Vol. XLVI (1895), pp. 325 *et seq.*

† Given implicitly first in *Mathematische Annalen*, Vol. XLIII (1893), pp. 329, 330.

‡ Frobenius, *Berliner Sitzungsberichte*, 1895, pp. 184, 185.

§ "Theory of Groups," 1897, p. 228.

|| *Philosophical Magazine*, Vol. CCXXXI (1908), pp. 223 *et seq.*

istic pair; in case the set consists of a single operator or subgroup, this is characteristic as already noted.

It results immediately from the fundamental property of a characteristic set of subgroups that *if G is the direct product of a characteristic set of subgroups, the I of G is the product of the groups of isomorphisms of these subgroups extended by operators corresponding to whatever isomorphisms are possible among these subgroups themselves.*

In the present discussion, unless the contrary is stated, the definition of a characteristic set of subgroups of G will be restricted to mean a single complete set of conjugate subgroups under the group of isomorphisms of G. A few special products will be considered, the different cases arising from different kinds of groups in the characteristic set.

THEOREM I. *If G is the n-th power of an indivisible group H whose central is the identity, then the I of G is the n-th power of the group of isomorphisms of H extended by operators which permute these n groups of isomorphisms according to the symmetric group of degree n. If i is the order of the group of isomorphisms of H, then the order of the I of G is $n!i^n$.**

For the proof of this theorem, as well as for the proof of a later theorem, it will be useful to have some auxiliary observations established. Accordingly, it will be shown first that *if G is the direct product of two indivisible groups G_1 and G_2, neither of which contains an invariant operator besides the identity, then G_1 and G_2 form a characteristic pair (according to the unrestricted definition).*†

In proving that G_1 and G_2 form a characteristic pair (or set), it is necessary and sufficient to show that neither G_1 nor G_2 can correspond to any subgroup containing operators outside this pair. Now G_1 and G_2 have the following properties: neither is divisible and neither contains an invariant operator besides the identity; every operator of one is commutative with each operator of the other; and their direct product is G. Since they have similar properties, it will suffice to show that G_1 could not, in any of the isomorphisms of G with itself, correspond to a subgroup outside this original pair. Suppose, if possible, that G' were a subgroup neither G_1 nor G_2 which could correspond to G_1 in some isomorphism of G. Since G_1 is not a direct product, G' could not be a direct product. Hence, this G' must be constructed by some isomorphism between

* By the "n-th power" is meant the direct product of n identical groups. An *indivisible* group is one which is not a direct product. *Divisible* is first used in English by Easton, "Constructive Development of Group Theory," 1902, p. 47, being a translation of "zerfallend," which was introduced by Dyck, *Mathematische Annalen*, Vol. XVII (1880), p. 482.

† Cf. Remak, *Crelle's Journal*, Vol. CXXXIX, (1910–11), pp. 293–308.

the original factor groups, or one of them and a subgroup of the other, or between invariant subgroups from both of them. Supposing that G' were formed by an $a:b$-isomorphism, it will be shown that it could not be simply isomorphic with G_1.

If G' were formed by an $a:b$-isomorpnism, then G_2 could not correspond to itself (because not all of its operators would be commutative with its constituents in G', since G_2 contains no invariant operator besides the identity), but must likewise have a G'' correspond to it in this particular isomorphism of G, and G'' would likewise be the result of some $a':b'$-isomorphism. Since every operator of G_1 is commutative with each operator of G_2, every operator of G' must be commutative with each operator of G'', and accordingly the constituents of G_1 found in the operators of G' must be commutative individually with the constituents from G_1 found in the operators of G'' (the same would be true respecting the constituents of G_2 as found in G' and in G''). From this fact it will now be shown that $[G', G'']$ would not contain G_1. From the conditions just stated about the commutability of constituents, if any constituent of G_1 in G' also appeared in G'', then G_1, if generated at all, would contain at least one invariant operator besides the identity; and if the constituents of G_1 in G' were all different from those in G'', then G_1 would be a direct product. But both results are contrary to the original hypothesis that G_1 contain no invariant operator besides the identity and be indivisible. Hence, $[G', G'']$ does not contain G_1, or, in other words, G is not generated by G' and G''. Therefore, in no isomorphism of G with itself can G_1 or G_2 correspond to a subgroup outside this generating pair, or G_1 and G_2 constitute a characteristic pair (or set) of subgroups of G.*

The development of this proof further shows that G can not be the direct product of another pair of indivisible groups neither of which contains an invariant operator besides the identity. Moreover, no factor of G could contain an invariant operator besides the identity, for then the central of G would not be the identity. Accordingly, if G is the direct product of two indivisible groups neither of which contains an invariant operator besides the identity, then if G can be represented as the direct product of two other factors, at least one of these must be divisible. If G were the product of several factors, the same line of proof would establish the generalization of this statement; viz.: *If G is the direct product of n indivisible groups $G_1, \ldots, G_n$ no one of which*

* If, in addition to the conditions already imposed upon G_1 and G_2, it is given that $g_1 \neq g_2$, then evidently G_1 and G_2 are themselves characteristic subgroups, and the I of G is the direct product of the groups of isomorphisms of these subgroups. Cf. Miller, *Transactions of American Mathematical Society*, Vol. I (1900), p. 396.

contains an invariant operator besides the identity, and if G can be represented as the direct product of other factors not all of which are identical with the former n, then at least one of this second set of factors is divisible. From this it is evident that if G were the product of n such indivisible groups, no outside subgroup could correspond to any of these in any automorphism of G; and accordingly the preliminary observation becomes: *If G is the direct product of n indivisible groups no one of which contains an invariant operator besides the identity, then these n groups form a characteristic set (according to the unrestricted definition).* *

To proceed with the proof of Theorem I, let $H_1, H_2, \ldots, H_n$ be the n similar groups each simply isomorphic with H, and let $I_1, I_2, \ldots, I_n$ be their respective groups of isomorphisms. These will also be simply isomorphic among themselves and have the same order i. Since $G \equiv [H_1, \ldots, H_n]$, G is invariant under each of these I's and hence under their direct product. Moreover, in each of the i^n different isomorphisms effected by $[I_1, \ldots, I_n]$ each of these n generating H's corresponds to itself. Now G is the direct product of the n indivisible groups no one of which contains an invariant operator besides the identity; hence, from the preceding observation no outside subgroup of G can correspond to any of the H's in any of the isomorphisms of G, or these n H's form a characteristic set.

From the fact that the original n generating H's constitute a characteristic set, the remaining isomorphisms of G are those arising when the n H's correspond among themselves; and this is possible, since they all are simply isomorphic and distinct. Now if an operator s_i of one of the H's, say H_i, corresponds to an operator s_j of H_j, then H_i and H_j must correspond in simple isomorphism throughout, because, since no H is a direct product nor contains an invariant operator besides the identity, and since no operator from outside the groups of the generating set can correspond to an operator of the generating set, evidently the operators of H_i are the only ones in the generating set which, with s_i, form a subgroup H which could be simply isomorphic with H_j. Hence, the correspondences among the n generating H's of the characteristic set can be effected in exactly $n!$ ways, corresponding exactly to the symmetric group of degree n.

The I of G, therefore, is of order $n!i^n$ and is simply isomorphic with $[I_1, I_2, \ldots, I_n]$ extended by operators which permute the I's according to the symmetric group of order $n!$.

* Cf. Remak, *loc. cit.*, p. 304.

Example. Suppose that $G \equiv (abcd)$ pos $(efgh)$ pos $(ijkl)$ pos. Then the I of G is $[(abcd)$ all $(efgh)$ all $(ijkl)$ all$] \cdot (eai \cdot bfj \cdot cgk \cdot dhl) \cdot (ae \cdot bf \cdot cg \cdot dh)$.

By means of this theorem it is easy to establish the following one on a system of groups of isomorphisms which are complete groups:

THEOREM II. *If H is the group of isomorphisms of a simple group S of composite order, then the I of the n-th power of H is a complete group of order $n!h^n$ which is the n-th power of H extended by operators which permute the n H's according to the symmetric group of degree n.*

In proving this theorem, use will be made of a proposition due to Burnside, "If G is a simple group of composite order, or if it is the direct product of a number of isomorphic simple groups of composite order, the group of isomorphisms L of G is a complete group." *

Since S is a simple group, it is indivisible and contains no invariant operator besides the identity. Hence, from Theorem I, the group of isomorphisms of the n-th power of S is $L \equiv [H_1, \ldots, H_n]$ extended by operators which permute the H's according to the symmetric group of degree n, and from Burnside's theorem, L is a complete group.

The quoted theorem states that H also is a complete group. It accordingly contains no invariant operator. Moreover, it is indivisible. To show this it will first be proved that *if a group which is the direct product of indivisible factors no one of which contains an invariant operator besides the identity, contains an invariant simple group, then that simple group is contained wholly in one of the factors.* For this simple group could not be the direct product of invariant subgroups from different factors, nor could it be the result of any isomorphism, not 1:1, of such subgroups from different factors, because in both cases the group formed would be composite. Since no factor contains an invariant operator besides the identity, the required group could not be the result of a 1:1-isomorphism, for in this case the group formed would not be invariant under the entire group. Hence, if an invariant simple subgroup occurs, it must be wholly in one of the factors.

Now to complete the proof that H is indivisible, suppose it were divisible. S is its own group of cogredient isomorphisms, and hence it is contained in H invariantly. Then from the statement just established, if H were divisible, S would necessarily be contained wholly in one of the factors. But this would lead to an absurdity, for then S would be transformed in the same way by more than one operator in its group of isomorphisms, since every operator of the other factors would transform it in exactly the same way as the identity.

* "Theory of Groups," 1911, p. 96.

Accordingly, H is an indivisible group. Then since H contains no invariant operator besides the identity and is indivisible, the preceding Theorem I can be applied to the n-th power of H, and the group of isomorphisms is seen to be $I \equiv [H_1, \ldots, H_n]$ extended by operators which permute the H's according to the symmetric group of degree n. Furthermore, since I is seen to be the same as the complete group L, I is likewise a complete group.

Example. The group of isomorphisms of the simple group of order 168 and degree 7 is known to be simply isomorphic with the group of order 336 and degree 8. Hence, the I of the n-th power of $(abcdefgh)_{336}$ is a complete group, which may as a substitution group be obtained according to the theorem.

COROLLARY I. *The I of the n-th power of a symmetric group whose degree is >4 and $\neq 6$ is a complete group.*

Because these symmetric groups are the groups of isomorphisms of their respective alternating groups which are simple and of composite order.*

COROLLARY II. *If H is the group of isomorphisms of a simple group S of composite order, then the I of the square of H or of S is a complete group which is the double holomorph of H.*

From the given theorem this I is seen to be the square of H extended by an operator of order 2 which interchanges the two systems. Since H is a complete group, the resulting I is the double holomorph of H.†

Again, in connection with the groups of isomorphisms of the squares of certain groups, another theorem which is closely related to the preceding two will be given.

THEOREM III. *If G is the square of an indivisible group H whose central is the identity and which is simply isomorphic with a characteristic subgroup of its group of isomorphisms, then the I of G is simply isomorphic with the double holomorph of the group of isomorphisms of H.*

In proving this theorem it may be supposed that H is written as a regular substitution group. Then the operators transforming it according to its possible automorphisms can be written as substitutions on the same letters.‡ Furthermore, since H contains no invariant operator besides the identity, and is thus its own group of inner isomorphisms, it is identical with the characteristic subgroup of its group of isomorphisms (I_H) with which it was known to be simply isomorphic. Since no two operators of the group of isomorphisms of a group transform that group in the same way, no operator besides the

* See Burnside, "Theory of Groups," 1911, §§ 162, 139.

† This term was introduced by Miller. See *Transactions of American Mathematical Society*, Vol. IV (1903), p. 154.

‡ Frobenius, *Berliner Sitzungsberichte*, 1895, pp. 184, 185.

identity in I_H can be commutative with all the operators of H. Hence, I_H contains no invariant operator besides the identity, or is its own group of inner isomorphisms.

Now H is a characteristic subgroup of I_H, and accordingly the possible automorphisms of I_H with the operators of H in some fixed correspondence form an invariant subgroup of the group of isomorphisms of I_H. But since no two operators in I_H and outside H transform the operators of H in the same way, the total automorphism of I_H is fixed if the automorphism of H is fixed. Hence, the I of the group of isomorphisms of H is not of greater order than is I_H itself. But its group of inner isomorphisms has been seen to be of that order. Accordingly, since I_H contains no invariant operator besides the identity and admits of no outer isomorphism, it is a complete group.*

Finally, from Theorem I the I of G is seen to be the square of a complete group extended by an operator of order 2 which interchanges the two systems, and therefore this G is the double holomorph of the group of isomorphisms of H.

Example. If $G \equiv (abcd)$ pos $(efgh)$ pos, then $I \equiv [\,(abcd)$ all $(efgh)$ all$]\cdot$ $(ae \cdot bf \cdot cg \cdot dh)$, which is the double holomorph of the symmetric group of degree 4.

This part of the discussion is concluded with the following theorem and corollaries on conjoints: †

THEOREM IV. *If an indivisible group H and its conjoint H' generate G, where the order of the central of H is not greater than 2, then if G contains no other pair of subgroups simply isomorphic with H and H', the I of G is simply isomorphic with the square of the group of isomorphisms of H extended by an operator of order 2 which simply interchanges the two systems.*

Suppose that C is the central of H. From the nature of the construction of the conjoints, C is also the central of H', and the cross-cut of the two groups; accordingly, it is the central of G. By hypothesis C is either the identity or the identity and a characteristic operator of order 2.

It will be proved that these two conjoints form a characteristic set or pair. Let the operators of H outside C be represented by s's, those of H' by t's; thus,

$$H \equiv C,\ s_2,\ s_3,\ \ldots,\ s_h;$$
$$H' \equiv C,\ t_2,\ t_3,\ \ldots,\ t_h.$$

Since by hypothesis there are no other pairs of subgroups which could correspond to H and H', it is sufficient to show that no subgroup exists in G

---

* Burnside gives a different proof (*loc. cit.*, p. 95).

† The term *conjoint* is due to Jordan. See "Traité des Substitutions," 1870, p. 60.

which could correspond to one of these conjoints and with the other form a generating pair in some automorphism of G. Any such subgroup would have to contain an operator or some operators from outside H and H'. But none of the operators outside H and H' is commutative with all the operators of H or with all those of H'. This is because all such operators are of the form $s_i t_j$ $(i, j = 2, \ldots, h)$, where neither factor is from the central of C; so that the product can not be commutative with all of $s_2, \ldots, s_h$ nor with all of $t_2, \ldots, t_h$. Accordingly, no subgroup exists which could replace either conjoint in an automorphism of G; so that, under the hypotheses, they constitute a characteristic pair of subgroups.

Since the operators of each conjoint are commutative with each operator of the other, and each conjoint subgroup is independent of the other, evidently each can correspond exactly according to its own group of isomorphisms while the other remains fixed in identical correspondence. Furthermore, the conjoints themselves can correspond, and they correspond throughout if some operator outside the central of one is in correspondence with an operator of the other. That is, if some s corresponds to some t, then H and H' correspond entirely. Otherwise, it would be possible to form from the operators of H and H' two groups each simply isomorphic with H, each containing both s's and t's, and they would possess the property that every operator of one was commutative with every operator of the other. Since H is not a direct product, this would necessitate that some one or more of the s's (or t's) be commutative with all the other s's (or t's), making the order of the central greater than that of C, which would be contrary to hypothesis. Hence, if one operator (outside C) of H corresponds to an operator of H', all of H corresponds to H'.

Hence, G has the isomorphisms of H, combined with all those of H', and finally those additional ones resulting from making H and H' correspond, and it has no more. The I of G is thus representable as a substitution group by extending the square of the group of isomorphisms of H by an operator which simply interchanges the two systems.

Should H contain no invariant operator besides the identity, from the auxiliary facts established in the proof of Theorem I, H and its conjoint would constitute a characteristic pair, and the conditions would be a special case of Theorem I with $n=2$; viz.:

COROLLARY I. *If G is generated by an indivisible group H and its conjoint H', where H contains no invariant operator besides the identity, then the I of G is simply isomorphic with the square of the group of isomorphisms of H extended by an operator of order 2 which simply interchanges the two systems.*

If, in this theorem or the corollary just stated, the group of isomorphisms of H should be a complete group, the I of G would be simply isomorphic with the double holomorph of the group of isomorphisms of H.

If two conjoints such as those of the theorem generate a group G which contains other pairs of simply isomorphic subgroups (which could correspond to H and H' in some automorphism of G), then from the preceding proof, where it was shown that no one subgroup could be in two different pairs of conjoints, the following statement can be made regarding the order of the group of isomorphisms of G:

COROLLARY II. *If G is generated by an indivisible group H and its conjoint H', where the order of the central of H is not greater than* 2, *then the order of the I of G is twice the product of the order of the group of isomorphisms of H by the number of pairs of subgroups which can correspond to H and H' in the automorphisms of G.*

Example. The group $G \equiv [(abcd)_8\,(efgh)_8]_{2,2}\,(ae \cdot bf \cdot cg \cdot dh)$, which is of degree 8, well illustrates most of the theory brought out in connection with this theorem. This group is generated by two conjoint quaternion groups having a common central (the identity and a characteristic operator of order 2) and nothing else in common; furthermore, it contains no other quaternion subgroups. Now the symmetric group of degree 4 is the group of isomorphisms of the quaternion group,* so that the I of G is simply isomorphic with the square of the symmetric group of degree 4 extended by an operator of order 2 which simply interchanges the two systems; or since the symmetric group of degree 4 is a complete group, this I is the double holomorph of this symmetric group, its order being 1152.

Again, it may be noted that this G is generated by a pair of conjoint octic groups. If there were but one pair, I would be of order 128; but there are nine distinct pairs of octic groups, each pair having the properties of conjoints and being generators of G; so that the I of G is of order $9 \times 128 = 1152$.

II. *Theorems on the Direct Product of Particular Dissimilar Groups.*

In the theorems of this section the group G is the direct product of two subgroups, one of which (A) is characteristic, and the other (B) may have conjugates under the group of isomorphisms (I_G). A and B, therefore, have the following properties: every operator of B is commutative with each operator of A; the identity is their only common operator; A and B generate G; A always corresponds to itself; and B may correspond to some other subgroup.

* Cf. Miller, *Bulletin of American Mathematical Society* (2), Vol. V (1898–99), p. 294.

Since A always corresponds to itself, any group B' which corresponds to B in any automorphism of G can have only the identity in common with A; hence, B' could not be the direct product of any subgroup from A and any subgroup of B. Accordingly, if B' exists, it must be formed by some isomorphism. Every operator of B' must be commutative with each operator of A; hence, any operators of A appearing as constituents in B' must be from the central of A. B' could not be formed by an isomorphism of any subgroup from B of index $\overline{\gtrless} 2$ with a subgroup from the central of A, for the group generated by such a group and A would not contain B, hence would not be G. Hence, since B' is to be of the same order as B, every possible B' must be formed by a $d{:}1$-isomorphism of B with some subgroup from the central of A. Such a group and A would evidently generate B and accordingly G; moreover, it would be simply isomorphic with G and would have only the identity in common with A. With this introduction the following auxiliary proposition will be established for immediate use in the following four theorems:

THEOREM V. *If the group G is the direct product of two groups A and B such that* (a) *A is characteristic in G;* (b) *B and all its conjugates contain a common subgroup D of index p (p being any prime);* (c) *the operators of order p in the central of A form a characteristic subgroup which admits of α-holomorphisms,* $\alpha = 1, \ldots, (p-1)$, under the I of A: then the I of G is simply isomorphic with the direct product of the group of isomorphisms of B (I_B) and a group I'.*

From the statement of the conditions it is obvious that all the conjugates of B are formed by a $d{:}1$-isomorphism between B and cyclic groups of order p from the central of A, all of these conjugates having the same head D, which is thus a characteristic subgroup of G. It will first be proved that the I of G is simply isomorphic with a group generated by I_A, I_B, and operators representing certain transformations of B into its conjugates. Ultimately it will be shown also that *I' is generated by the group of isomorphisms of A (I_A) and operators corresponding to the transformation of B into its conjugates in which the order of the B-constituents is the same as the order of the operators of B itself.*

In the automorphisms of G, A can correspond according to all its possible isomorphisms while B remains in identical correspondence, and *vice versa.* But each such set of transformations forms a group, I_A and I_B, respectively, which have nothing more than the identity in common. Hence, the I of G has

* Defined by Young (J. W.), *Transactions of American Mathematical Society,* Vol. III (1902), p. 186.

subgroups simply isomorphic with I_A and with I_B (all the operators of one subgroup being commutative with each of those of the other) and a subgroup simply isomorphic with their direct product. When referring to these simply isomorphic subgroups, they will be called I_A, I_B, etc., rather than "the subgroup simply isomorphic with I_A," etc. With the characteristic subgroup A in identical correspondence, B can correspond to itself according to I_B and can correspond to each of its conjugates. Thus, the group generated by I_B and operators corresponding to the transformation of B into its conjugates is an invariant subgroup of the I of G, and since the quotient group is the I_A, and the I of G is known to contain I_A, none of whose operators (excepting the identity) is in the invariant subgroup, therefore the I of G is generated by I_A, I_B, and operators representing the transformation of B into its conjugates.

It will now be proved that the I of G contains a subgroup, simply isomorphic with I_B, every operator of which is commutative with the operators effecting the automorphisms of A and the transformation of B into its conjugates leaving the order of the operators of B unchanged as they become constituents of a B'.

Suppose that $m-1$ subgroups can be formed to correspond to B (besides itself). D, the characteristic head of all these conjugates, and any one of the m tails form a group simply isomorphic with B. Since p is a prime, the co-sets with respect to D in B (or in a B') are transformed among themselves cyclically if they are permuted at all; and if the co-sets of one conjugate are permuted, the corresponding co-sets of all the conjugates permute in the same order. Consider an operator which transforms B into itself according to some one of its automorphisms. If each one of the following $m-1$ tails does not go into itself under this transformation of the operators of B, a different transforming operator can be found which will effect the same automorphism of B and simultaneously transform each tail into itself. Such an operator can be found by taking the product of the original transforming operator by an operator from I_A which effects the same n-holomorphism among the operators of order p in A's central as is effected by the original transforming operator among the co-sets of the tail of B. If R is such an operator of the I of G, and any operator of B, as t_1 (which for convenience may be supposed in the first co-set after D), is transformed into t'_n in the n-th co-set (where $n=1, \ldots, \overline{p-1}$, supposing that the order of the co-sets is that of successive powers), and if c is an operator of order p from the central of A, then

$$R^{-1} t_1 r = t'_n \qquad (R^{-1} cR = c^n). \tag{1}$$

Now let V be any operator of the I of G which transforms B into a B' leaving

the order of the B-constituents the same as that of the corresponding operators of B. Then

$$V^{-1}t_1V=t_1c^i \qquad (V^{-1}t'_nV=t'_nc^{ni}). \tag{2}$$

Transforming (1) by V and (2) by R gives

$$V^{-1}R^{-1}t_1RV=V^{-1}t'_nV=t'_nc^{ni},$$
$$R^{-1}V^{-1}t_1VR=R^{-1}t_1c^iR=t'_nc^{ni}.$$

Hence, $VR=RV$. But the totality of the R's constitute a subgroup of the I of G simply isomorphic with I_B. Accordingly, each operator of this R-subgroup is commutative with each operator transforming B into a B', under the conditions stated.

It must also be shown that every R is commutative with the operators effecting the automorphisms of A. The only automorphisms of A which need be examined in this relation are those affecting the c's in some way. If W is an operator effecting some such automorphism of A, it is commutative with t; hence, WR and RW transform B in exactly the same way. Suppose that

$$W^{-1}cW=c' \qquad (W^{-1}tW=t)\,; \tag{3}$$

then, from (1) and (3),

$$R^{-1}W^{-1}cWR=c'^n,$$
$$W^{-1}R^{-1}cRW=c'^n.$$

Hence, the R's are individually commutative with the operators of I_A; and, accordingly, there is in the I of G a factor which is simply isomorphic with I_B.

Since the I_B is a factor, the other factor (I') depends only upon the isomorphisms of A and those of the tails. Hence, in determining I', the operators of B can be used in some arbitrary order. If letters be placed before each of the $m(p-1)$ co-sets of the m tails with respect to D (a letter before each such co-set), and letters before such operators of A outside its largest characteristic subgroup (none are needed if all the operators are commutative and of order p) as are necessary to determine its group of isomorphisms, then the permutations of these letters during the transformation of B into each B' (B-constituents remaining in the same order as the corresponding operators of B itself), and during all the automorphisms of A, will determine I'.

In the following theorems A and B are of such forms that I' is readily obtained.

NOTES. If in this proposition $p=2$, then the proof is much simpler, since there is but one co-set in each tail and hence no cyclical permutation of the co-sets in any tail.

If, in addition to the given hypotheses, the central of A is known to be the identity, then B also is characteristic and the I of G immediately determined. Or, if B contains no invariant subgroup whose quotient group is simply isomorphic with a subgroup of the central of A, then B also is characteristic and the I of G determined as before.*

---

* Miller, *Transactions of American Mathematical Society*, Vol. I (1900), p. 396.

Example. If $G \equiv (abcd)$ all $(efgh)_8$, then A is the octic group, B is the symmetric group $(abcd)$ all, and there is but one B', which is formed by dimidiating B with the central of A. The operator of order 2 which transforms B into B' is commutative not only with all the operators of I_B but also with those of I_A (because the operator of order 2 from A used in the dimidiation is characteristic in A and invariant under I_A). Therefore, the I of G is simply isomorphic with $(abcd)$ all $(efgh)_8(ij)$.

The following theorem is stated because it represents the common starting point of Theorems VII, VIII, IX and X, which follow; and a proof is here given to introduce the method of demonstration to be employed throughout. The latter four theorems are extensions in different directions of the one under immediate consideration.

THEOREM VI. *If a group G is the direct product of the group of order p, p being any prime, and a group H which contains a characteristic subgroup D of index p, neither D nor the central of H containing an invariant subgroup of index p, then the I of G is simply isomorphic with the direct product of the group of isomorphisms of H and the holomorph of the group of order p.*

The cyclic group of order p is characteristic, since it is the only subgroup of order p in the central of G; and since D is characteristic in H and contains no invariant subgroup of index p, it too is characteristic in G. Each of these subgroups must correspond to itself in every isomorphisms of G; furthermore, G must contain the product of these two subgroups as a characteristic subgroup of index p. After this characteristic subgroup of index p is fixed in any isomorphism, there can correspond to any one of the remaining co-sets, with respect to D, any one of p such co-sets and no more, and this correspondence then establishes the isomorphism of the entire group. The I of G thus contains an invariant cyclic subgroup of order p. For convenience, it may be supposed to be of degree p, a letter corresponding to each of the p interchangeable co-sets. Now, if the operators of the characteristic subgroup D are retained in the same isomorphism as before, there are exactly $p-1$ possible correspondences of the succeeding co-sets in the characteristic subgroup of index p, since any one of the $p-1$ co-sets can stand first and the order of the remaining ones is then determined. I thus contains an invariant subgroup of order $p(p-1)$ which, moreover, contains the cyclic subgroup of order p invariantly. Since this subgroup can be written on p letters, it is the holomorph of the cyclic group of order p.

The only other isomorphisms of G are those effected by the group of isomorphisms of H, and accordingly, from Theorem V, the I of G is simply

isomorphic with the direct product of the group of isomorphisms of H and the holomorph of the cyclic group of order p.

Example. If $G \equiv (abcd)$ pos (efg) cyc, then H is the alternating group $(abcd)$ pos which contains a four-group as a characteristic subgroup D of index 3, neither D nor the central of H containing an invariant subgroup of index p. Since the group of isomorphisms of this H and the holomorph of the cyclic group of order 3 are known, the I of G is simply isomorphic with $(abcd)$ all (efg) all.*

THEOREM VII. *If a group G is the direct product of an abelian group A of order p^m, type $(1, 1, 1, \ldots.)$, p being any prime, and a group H which contains a characteristic subgroup D of index p, neither D nor the central of H containing an invariant subgroup of index p, then the I of G is simply isomorphic with the product of the group of isomorphisms of H and the holomorph of A.*

The abelian group A is characteristic in G, since it is the largest subgroup in the central of G that contains operators of order p only; and since D is characteristic in H and contains no invariant subgroup of index p, it too is characteristic in G. Each of these subgroups must correspond to itself in every automorphism of G; furthermore, G must contain the product B of these two subgroups as a characteristic subgroup of index p. The rest of G consists of the product of the abelian group A into the tail of H (which is H minus D).

Suppose, while determining the isomorphisms of the various subgroups which can be formed by isomorphism, that the operators of H remain in some fixed order. Let the characteristic subgroup B be in some identical correspondence; then any one of the first p^m co-sets in the tail of G can be taken to correspond with the one originally first. When this is selected, it with B determines the entire isomorphism of G. There are, accordingly, exactly p^m such isomorphisms, and they are commutative and each of order p. Hence, so far as the isomorphisms of these subgroups of G are concerned, there is an invariant abelian subgroup of order p^m, type $(1, 1, 1, \ldots.)$. For convenience, this subgroup may be supposed to be written on p^m letters, one corresponding to each of the first p^m co-sets formed with respect to D, since the p^m co-sets of any of the $p-1$ systems of similar co-sets correspond among themselves and only among themselves, excepting in isomorphisms of H itself.

Next, consider the possible isomorphisms of the co-sets in B (the operators of H being in the same original order, and D thereby in identical corre-

* Cf. Miller, *Philosophical Magazine*, Vol. CCXXXI (1908), pp. 223 *et seq.*

spondence). The arrangement of these co-sets is unrestricted by the order of the co-sets in the tail of G ($=G$ minus B). Hence, since these p^m-1 co-sets differ from one another only by operators from A by which D is multiplied to give them, they may be made isomorphic exactly according to the group of isomorphisms of A.

This then effects all the possible isomorphisms of A and of the p^m subgroups simply isomorphic with H (found by a $d:1$-isomorphism of H with each of the $\frac{p^m-1}{p-1}$ subgroups of A,* each of order p and each being here employable in $p-1$ ways, since any one of its operators of order p can be taken as the generator). The number of these isomorphisms is p^m times the order of the group of isomorphisms of A. Furthermore, the group of these isomorphisms can be written on the p^m letters previously introduced, and it contains as an invariant subgroup, as was seen, an abelian group of order p^m, type $(1, 1, 1, \ldots.)$. But p^m times the order of the group of isomorphisms of A is the order of the holomorph of A, which is the maximum group on p^m letters containing A invariantly. Hence, this group is the holomorph of A.

Besides these isomorphisms already determined, the only other isomorphisms of G are those effected by the group of isomorphisms of H, and from Theorem V this group is a factor in the I of G. Therefore, the I of G is simply isomorphic with the direct product of the group of isomorphisms of H and the holomorph of A.

Example. If $G\equiv(abcd)$ all $(ef)(gh)$, then H is the symmetric group of degree 4 and A is the four-group. Since H is then a complete group and the holomorph of the four-group is the symmetric group of order 24, the I of G is simply isomorphic with $(abcd)$ all $(efgh)$ all.

The groups of isomorphisms of abelian groups of order p^m, type $(1, 1, 1, \ldots.)$, have been studied by Moore,† so that the holomorph of such a group is a definitely determined group. When $p=2$, it is interesting to note that, if $m=2$ (A is then the four-group), the holomorph is the symmetric group of order 24; if $m=3$, the holomorph of A is the group of order 1344 and degree 8; ‡ if $m=4$, the holomorph of A is a primitive substitution group of degree 16, order $8!8$.§

* Burnside, "Theory of Groups," 1911, p. 110.

† Moore, *Bulletin of American Mathematical Society* (2), Vol. II (1895), pp. 33–43. Cf. Burnside, "Theory of Groups," 1911, §§ 89, 90.

‡ For more information and references on this interesting group see Miller, AMERICAN JOURNAL OF MATHEMATICS, Vol. XXI (1899), p. 337.

§ Miller, AMERICAN JOURNAL OF MATHEMATICS, Vol. XX (1898), p. 233.

COROLLARY. *If G is the direct product of a symmetric group of degree n, $n \neq 2$ nor 6, and an abelian group of order 2^m, type $(1, 1, \ldots .)$, then the I of G is simply isomorphic with the direct product of that symmetric group and the holomorph of the given abelian group.*

*If $n=2$, G is simply an abelian group of order 2^{m+1}, type $(1, 1, \ldots .)$. If $n=6$, the I of G is the direct product of the holomorph of the given abelian group and an imprimitive group of order 1440 and degree 12, this being the group of isomorphisms of the symmetric group of order 720.**

THEOREM VIII. *If a group G is the direct product of a cyclic group of order p^m, p being an odd prime, and a group H which contains a characteristic subgroup D of index p, neither D nor the central of H containing an invariant subgroup of index p, then the I of G is simply isomorphic with the direct product of the cyclic group of order p^{m-1}, the holomorph of the group of order p, and the group of isomorphisms of H.*

From the hypotheses, D is characteristic in G, as is also the cyclic group (E) of order p^m and the single subgroup of order p contained in it, these latter two being the only subgroups of their respective orders in the central of G. From Theorem V, the I of G will be the direct product of the group of isomorphisms of H and a group I' which is generated by the group of isomorphisms of the cyclic group and operators corresponding to the subgroups to which H can correspond. It remains to determine I'.

Now G is generated by the characteristic cyclic group of order p^m and H or any group simply isomorphic with H which can be formed by an isomorphism of H with subgroups from E. The only subgroup from E which can be thus used is the single one of order p, since D is the subgroup which in H must be employed as the invariant subgroup, and any subgroup of order greater than p from E would then result in a group of order greater than H, which then could not be put into simple isomorphism with it. Since this subgroup of order p can be generated by any one of its $p-1$ operators of order p, H and the $p-1$ different groups which can be formed simply isomorphic constitute a characteristic set of p subgroups; and with E in fixed isomorphism, the resulting invariant subgroup in I' is a cyclic group of order p.

The group of isomorphisms of E is a cyclic group of order $\phi(p^m) = p^{m-1}(p-1)$.† In this the operators of order p^n, $n=1, \ldots, m-1$, leave the

* Miller, *Bulletin of American Mathematical Society* (2), Vol. I (1895), p. 258; and Hölder, *Mathematische Annalen*, Vol. XLVI (1895), p. 345.

† Burnside, "Theory of Groups," 1911, § 88; also Miller, *Transactions of American Mathematical Society*, Vol. IV (1903), pp. 153–160.

operators of order p in E invariant, simply transforming among themselves in the possible ways the operators of order p^i, $i>1$, in E whose first power in the subgroup of order p is the same operator. Since these operators of order p are invariant under this cyclic group of order p^{m-1}, the subgroup of order p in I' will have each of its operators commutative with each of the operators of this cyclic group. But the cyclic subgroup of order $p-1$ in the group of isomorphisms of E transforms the cyclic subgroup of order p in E exactly according to its possible isomorphisms, or the cyclic subgroup of order p in I' is transformed according to its own group of isomorphisms. Hence, I' contains a cyclic group of order p^{m-1} and a cyclic group of order p extended by operators transforming it into all its possible isomorphisms, these operators being commutative individually with those of the cyclic group of order p^{m-1}. Therefore, I' is the direct product of the cyclic group of order p^{m-1} and the holomorph of the group of order p.

If the cyclic group E were of order 2^m, then its group of isomorphisms would be an abelian group of order 2^{m-1}, type $(m-2, 1)$.* The operator of order 2 used from E in forming the only conjugate of H would be characteristic, hence unaffected by any operator of the group of isomorphisms of E. Accordingly, I' would be an abelian group of order 2^m, type $(m-2, 1, 1)$, and the theorem would be:

THEOREM IX. *If a group G is the direct product of a cyclic group of order 2^m and a group H which contains a characteristic subgroup D of index 2, neither D nor the central of H containing an invariant subgroup of index 2, then the I of G is simply isomorphic with the direct product of an abelian group of order 2^m, type $(m-2, 1, 1)$ and the group of isomorphisms of H.*

Example. If $G \equiv (abcd)$ all $(efgh)$ cyc, then $H \equiv (abcd)$ all contains the tetrahedral group as a characteristic subgroup D of index 2, neither D nor the central of H having an invariant subgroup of index 2. The I of G, accordingly, is simply isomorphic with $(abcd)$ all $(ef)(gh)$.

NOTE. It may be noted that in the preceding Theorems VI, VII, VIII and IX the fact that I_H is a factor in the I of G could be established in each case independently of the Theorem V. The problem is simple if $p=2$. If p is an odd prime, then in each case there is a holomorph of an abelian group of odd order p^m, type $(1, 1, \ldots.)$, which holomorph is a complete group.† By showing that this holomorph is an invariant subgroup of the I of G, it is known to be a factor.‡

THEOREM X. *If G is the direct product of the group of order 2 and a group H which contains in a characteristic series§ n successive subgroups*

* See preceding foot-note references.

† Burnside, "Theory of Groups," 1897, p. 239.

‡ Hölder, *Mathematische Annalen*, Vol. XLVI (1895), p. 325.

§ Defined by Frobenius, *Berliner Sitzungsberichte*, 1895, p. 1027.

each of index 2 *in the preceding, neither the last,* H_n *of index* 2^n *in* H, *nor the central of* H *containing an invariant subgroup of index* 2, *then the* I *of* G *is simply isomorphic with the direct product of the group of isomorphisms of* H *and an abelian group of order* 2^n, *type* $(1, 1, \ldots .)$.

While this theorem does not come directly under the problem considered in Theorem V, still it is easy to show that I_H is here a factor in the I of G. As suggested in a note after Theorem V, since the prime is 2, there is but one co-set outside the characteristic subgroup of index p in any subgroup of the characteristic series. Hence, there is no cyclic permutation among the co-sets of a tail, and in transforming H into any of its conjugates an operator (t) either goes into some operator (t') of the same co-set (or head) or goes into such an operator (t') multiplied by the operator of order 2. If one operator of a co-set is multiplied by one of the operators from the group of order 2, all of the operators of that co-set are multiplied by that same operator; say by c. Let R be an operator transforming H according to any one of its automorphisms; then

$$R^{-1}tR=t', \qquad (R^{-1}cR=c). \tag{1}$$

If V be an operator transforming H into any one of its conjugates without altering the order of the H-constituents from that of the order of the corresponding operators of H, then

$$V^{-1}tV=tc, \qquad (V^{-1}t'V=t'c). \tag{2}$$

Transforming (1) by V and (2) by R gives, respectively,

$$V^{-1}R^{-1}tRV=t'c,$$
$$R^{-1}V^{-1}tVR=t'c.$$

Hence, $VR=RV$, and I_H is accordingly a factor in the I of G. Since the group of isomorphisms of the group of order 2 is the identity, it remains only to determine the possible isomorphisms of H with its conjugates when the order of the H-constituents is the same as the order of the corresponding operators of H itself.

The operator of order 2 in the group of order 2 is characteristic in G. H_n is a characteristic subgroup of G. Let the operators of H be in some fixed order and let H_n remain in identical correspondence while the subgroup I' of the I of G is determined. Each isomorphism of H with an H' is fixed by n correspondences, one for each of $H, H_1, \ldots, H_{n-1}$, and there are two options in each case (since there are two conjugates in each case). These n correspondences are independent of one another, so that there are in all 2^n subgroups in this set of conjugates (including H itself). Moreover, the operator trans-

forming H into any of these H''s is of order 2, and all such transformations are commutative. Hence, I' is an abelian group of order 2^n containing no operator of order greater than 2. Therefore, the I of G is simply isomorphic with the direct product of an abelian group of order 2^n, type $(1, 1, \ldots.)$, and the group of isomorphisms of H.

Example. If $G \equiv (abc)$ all (def) all (gh), then $H \equiv (abc)$ all (def) all, in which $H_1 \equiv [(abc)$ all (def) all$]$ pos, which is a characteristic subgroup of index 2; $H_2 \equiv (abc)$ cyc (def) cyc, which is a characteristic subgroup of index 2^2 in H, and neither H_2 nor the central of H contains an invariant subgroup of index 2. Since the group of isomorphisms of H is the double holomorph of the symmetric group of order 6, or is $(abcdef)_{72}$, therefore the I of G is seen to be simply isomorphic with $(abcdef)_{72}\,(ghij)_4$.

THEOREM XI. *If G is the direct product of a metabelian group of order $p(p-1)$ and a cyclic group of order $p-1$, then the I of G is simply isomorphic with the direct product of the holomorphs of the cyclic groups of order p and $p-1$.*

The problem is insignificant if p is the even prime; hence, p will be supposed in the following proof to be an odd prime.

G contains the cyclic group (C) of order $p-1$ as a characteristic subgroup, since it is the central of the direct product. The metacyclic group (M) of order $p(p-1)$ is a complete group, being the holomorph of the cyclic group of order p,* which cyclic group is a characteristic subgroup of M. In the automorphisms of G, M corresponds to itself and to conjugates formed by multiple isomorphism of M with C and with all its various subgroups.

The conditions are not exactly those named in Theorem V, since here the characteristic subgroup of order p in M is not usually (only when $p=3$) of prime index. It must be noted, however, that this same characteristic subgroup of index $p-1$ occurs in all the conjugates of M and that the transformations of the co-sets of M are always cyclic with respect to this subgroup of index $p-1$. Accordingly, by means of equations like those employed in proving Theorem V, it can be shown immediately that the I of G contains the group of isomorphisms of M as a factor, the other factor (I') being the group of isomorphisms of the cyclic group of order $p-1$ extended by operators corresponding to the transformation of M into its conjugates without changing the order of the operators of M as they become constituents in the conjugates. Since M is its own group of automorphisms, it remains to show that I' is the holomorph of the cyclic group of order $p-1$.

* Burnside, "Theory of Groups," 1897, p. 239.

Now every subgroup of a cyclic group is cyclic and characteristic. If the order of any subgroup (including the identity and the given cyclic group itself) is d, it has exactly $\phi(d)$ automorphisms, so that the number of conjugates of M is $p-1$; because, from number theory, "If $d_1, d_2, \ldots, d_r$ be the different divisors of m,

$$\sum_{j=1}^{r} \phi(d_j) = |m|.\text{"}^*$$

If M is transformed into the conjugate formed by a multiple isomorphism between M and the cyclic group of order $p-1$ itself, the transforming operator is seen to be of order $p-1$; and, furthermore, if this transformation be repeated, it gives the entire set of $p-1$ conjugates. Accordingly, the subgroup in I' which corresponds to the transformation of M into all its conjugates (order of M-constituents being the same as the order of the operators of M) is a cyclic group of order $p-1$, which can be written as a transitive substitution group on $p-1$ letters, a letter corresponding to each conjugate. If the operators of M remain in some fixed order and the characteristic cyclic group of order $p-1$ in G is transformed according to its group of isomorphisms, the $p-1$ conjugate subgroups (in the set with M) are permuted according to this group of isomorphisms. Hence, the $p-1$ subgroups are permuted according to a group generated by a cyclic group of order $p-1$ and the group of isomorphisms of a cyclic group of order $p-1$. This group can be represented on $p-1$ letters and contains the cyclic group of order $p-1$ invariantly. Accordingly, I' is the holomorph of the cyclic group of order $p-1$, and the I of G is simply isomorphic with the direct product of the holomorph of order $p(p-1)$ and the holomorph of the cyclic group of order $p-1$.

Example. Let $G \equiv (abcde)_{20}\,(fghi)$ cyc. Then the metacyclic group is $M \equiv (abcde)_{20}$, which is the holomorph of the group of order 5. The holomorph of $(fghi)$ cyc is an octic group. Hence, the I of G is simply isomorphic with $(abcde)_{20}\,(fghi)_8$.

III. *Theorems on Some Extended Groups.*

THEOREM XII. *Suppose the group H written as a regular substitution group and its group of isomorphisms I_H written on the same letters. If H be extended by an invariant substitution of order* 2 *from I_H such that it transforms every operator of the central C of H into its inverse*† *and leaves H characteristic in the newly formed group G, then the I of G is simply isomorphic with the substitution group generated by C and I_H.*

The order of the I of G equals the product of the order of C by the order of I_H.

* Lucas, "Théorie des Nombres," 1891, p. 400.

† Miller, *Transactions of American Mathematical Society*, Vol. X (1909), pp. 471–478.

Since H is characteristic in G, when H is fixed in identical correspondence, the possible isomorphisms of the latter half of G determine an invariant subgroup of I. If s is the operator of order 2 by which H is extended, the products of s by each of the operators of C transform H exactly as s itself does, and all these products are of order 2; moreover, these are the only ones having these properties. Furthermore, the automorphisms which are effected if they in turn stand in correspondence with s, exactly correspond to a group (invariant in I) simply isomorphic with C.

The other possible isomorphisms arise when the subgroup H corresponds to itself in all the ways it may as a subgroup of G, which evidently could not be more ways than if it were an independent group by itself. But here it can correspond exactly according to its own group of isomorphisms, since its group of isomorphisms always transforms it into itself, and at the same time, by hypothesis, transforms s into itself. Hence, G is invariant under the group of isomorphisms I_H, and the order of the I of G equals the product of the order of C by the order of I_H, since the quotient group of I with respect to a group simply isomorphic with C has been seen to be I_H. Now, in the isomorphisms of G the operator s and its $c-1$ conjugates were first permuted according to an invariant subgroup (of I) simply isomorphic with C, and then exactly as the operators of C itself were permuted by the substitutions of I_H; moreover, these and their products are the only permutations of these c conjugates. Hence, the invariant subgroup (in I) simply isomorphic with C is transformed by the rest of the operators of I in exactly the same way as C is transformed by I_H. Now the first power of any operator of I_H appearing in C is the identity; otherwise some non-identity operator of I_H would transform H in the same way as the identity itself does, which is impossible. Moreover, C is invariant under I_H, since it is a characteristic subgroup of H. Hence, if C were extended by the operators of I_H, the resulting group would be of order equal to the order of I. With respect to the invariant subgroup C, its quotient group would be simply isomorphic with I_H. In this group, C is transformed exactly as the simply isomorphic invariant subgroup in I is transformed; also every operator of this group represents a different isomorphism of G. Hence, the group formed would be simply isomorphic with the I of G.*

NOTES. If, in the preceding theorem, H were the direct product of the group C (abelian) and a group (which could contain no invariant operator besides the identity), then the I of the extended group (G) would be simply isomorphic with the direct product of the holomorph of C and the group of isomorphisms of the other factor.

If the central C of H contained no operator of even order, then the substitutions of C would actually transform the c conjugates (of s) according to the group said to be simply isomorphic with C, and simultaneously leave H fixed in identical correspondence. In this case $[C, I_H]$ is a substitution group simply isomorphic with I and on the same letters as G, so that its operators actually transform G according to all its automorphisms.

* Miller, *Bulletin of American Mathematical Society* (2), Vol. III (1896–97), p. 218, Th. II.

The fact that I is here written as a regular group makes the method for obtaining the I of G seem formidable; still, since the central C frequently is of low order, a group simply isomorphic with the I of G can often be easily constructed.* That is, *if G is formed by extending a group H by an operator of order 2 which transforms each operator of the central (C) of H into its inverse and leaves H characteristic in G and such that it can still correspond to itself according to its own group of isomorphisms (I_H), then the I of G is simply isomorphic with the group obtained by extending a group C', simply isomorphic with C, by the operators of a group simply isomorphic with I_H, which operators transform C' exactly as the corresponding operators of I_H transform C, their first powers appearing in C' being the identity.*

Thus, if $H \equiv (abc)$ cyc $(defg)_8$, it is of order 24, its central $C \equiv (abc)$ cyc $(df \cdot eg)$ being a cyclic group of order 6, and its group of isomorphisms simply isomorphic with the direct product of an octic group and a group of order 2.† Suppose H is extended by an operator of order 2, say ab, which transforms each operator of C into its inverse; then H remains characteristic in the newly formed group G (since H is generated by the operators of G whose orders are divisible by 3). Hence, the I of G is simply isomorphic with a group generated by a cyclic group of order 6 and a group simply isomorphic with I_H (under which that cyclic group is invariant) which transforms the operators of that cyclic group into their inverses and is such that the first power of any of its operators appearing in that cyclic group is the identity. These conditions are fulfilled by $[(abc)(de)]\,[(ab)(fghi)_8]$. This is the group (abc) all $(de)(fghi)_8$, or I is simply isomorphic with the direct product of G and a group of order 2.†

Now if A is any abelian group of even order, it may be extended by an operator of order 4 which has its square in A and which transforms each operator of A into its inverse; all of the operators in the extension will be of order 4, and all have a common square in A. In connection with the preceding theorem, accordingly, the following proposition is obvious, since its proof is precisely as that just made:

If G is formed by extending a group H, whose central C is of even order, by an operator of order 4 whose square is in C and which transforms each operator of C into its inverse and leaves H characteristic in G and such that it can correspond according to its own group of isomorphisms (I_H), then the I of G is simply isomorphic with the group obtained by extending a group C' simply isomorphic with C, by the operators of a group simply isomorphic with

* Miller, *Bulletin of American Mathematical Society* (2), Vol. III (1896–97), p. 218, Th. II.

† Miller, *Philosophical Magazine*, Vol. CCXXXI (1908), pp. 231, 232.

I_H, which operators transform C' exactly as the corresponding operators of I_H transform C, their first powers appearing in C' being the identity.

If H is an abelian group, it is its own central, and the extended group G is in one case the general dihedral group and in the other the general dicyclic group. Theorems regarding the groups of isomorphisms in these special cases have been established by Miller; thus: *

1. *If an abelian group H which involves operators whose orders exceed 2 is extended by means of an operator of order 2 which transforms each operator of H into its inverse, then the group of isomorphisms of this extended group is the holomorph of H.*

2. *The group of isomorphisms of the general dicyclic group as regards an abelian group which is not both of order 2^m and type $(2, 1, 1, \ldots .)$, is the holomorph of this abelian group.*

The following theorem and its corollary cover cases of certain extensions of groups which contain no invariant operators besides the identity:

THEOREM XIII. *If a group H, whose central is the identity, is a characteristic subgroup of a group G which is simply isomorphic with an invariant subgroup of the group of isomorphisms of H (I_H), then the I of G is simply isomorphic with I_H.*

In proving this theorem it may be supposed that H is written as a regular substitution group and that I_H is written on the same letters. Since H is its own group of inner isomorphisms, it will be an invariant subgroup of the substitution group I_H, and will be a characteristic subgroup of an invariant subgroup G' of I_H, where G' is simply isomorphic with G. Abstractly, G and G' have the same group of automorphisms.

Since H is characteristic in G', the I of G will contain an invariant subgroup corresponding to the possible isomorphisms of G' when the operators of H remain in fixed correspondence. But H is extended by operators of its own group of isomorphisms to form G', and as these operators all transform H differently, this invariant subgroup is just the identity. Hence, the I of G' can not be greater than the group of isomorphisms of H. But G' is invariant under the group of isomorphisms of H and is transformed differently by each operator of this group. Therefore, the I of G is simply isomorphic with the group of isomorphisms of H.

Example. If $H \equiv (abcd)$ pos $(efgh)$ pos, then its group of isomorphisms is the double holomorph of the symmetric group of degree 4; viz., $(abcd)$ all

* Miller, *Philosophical Magazine*, Vol. CCXXXI (1908), pp. 224, 225.

$(efgh)$ all $(ae \cdot bf \cdot cg \cdot dh)$. H is a characteristic subgroup of $G \equiv [(abcd)$ all $(efgh)$ all$]$ pos, which is invariant in the double holomorph of the symmetric group of degree 4. Hence, the I of G is the double holomorph $(abcd)$ all $(efgh)$ all $(ae \cdot bf \cdot cg \cdot dh)$.

COROLLARY. *If the group of inner isomorphisms of a group H, whose central is the identity, is a characteristic subgroup of the group of isomorphisms of H (I_H), then the I of any group G which contains H, and which is simply isomorphic with an invariant subgroup of I_H, is simply isomorphic with I_H.*

If H is written as a regular group, I_H can be written on the same letters and will contain H as a characteristic subgroup. Hence, I_H is a complete group (see proof of Theorem V), and accordingly contains no other subgroup simply isomorphic with H. For this reason H is characteristic in any subgroup of I_H, or is characteristic in G. The rest of the proof follows from the preceding theorem.

Example. If H is the dihedral group $[(abcde)_{10}\,(fgh)$ all$]$ dim, order 30, its group of isomorphisms is the double holomorph of the cyclic group of order 15, or $I_H \equiv (abcde)_{20}\,(fgh)$ all, order 120. Now H contains no invariant operator besides the identity and is characteristic in I_H, because it is formed by the group G_{15} composed of all the operators of orders 3, 5 and 15 and every operator of order 2 (in I_H) which transforms each operator of G_{15} into its inverse. Hence, since any subgroup of index 2 in I_H is an invariant subgroup, $(abcde)_{10}\,(fgh)$ all, which is of order 60 and contains H, has I_H for its group of isomorphisms.